

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

REMARKS

The foregoing amendment is filed in response to the official action dated January 13, 2006. Reconsideration is respectfully requested.

The status of the claims is as follows:

Claims 1-25 are currently pending.

Claims 1-25 stand rejected.

Claims 1, 13, 21, and 25 have been amended.

Claims 3-4 and 15-16 have been canceled without prejudice.

The Examiner has rejected claims 1, 3-8, 10-13, 15-20, and 22-25 under 35 U.S.C. 102(e) as being anticipated by Staveley et al. (USP 6,973,491). The Applicant respectfully submits, however, that amended base claims 1, 13, and 25 and the claims dependent therefrom are not anticipated by the art of record. For example, amended claim 1 recites a distributed method for performing network monitoring that includes the steps of (1) obtaining, by an infrastructure management appliance connected to a customer network, customer specific information from a remote data center connected to a public network, in which the customer network is connectable to the public network, and in which the customer specific information is obtained from the remote data center over a first interface to the infrastructure management appliance, (2)

-12-

WEINGARTEN, SCHURGIN,
GARDNER & LEBOVITZ LLP
TEL. (617) 542-2290
FAX. (617) 451-0323

BEST AVAILABLE COPY

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

establishing, by the infrastructure management appliance, a secure virtual connection with the remote data center, in which the establishing of the secure virtual connection with the remote data center is responsive to the customer specific information obtained from the remote data center over the first interface to the infrastructure management appliance, and in which the establishing of the secure virtual connection with the remote data center is performed over the public network over a second interface to the infrastructure management appliance, (3) monitoring, by the infrastructure management appliance, at least one customer resource connected to the customer network over the customer network, and (4) transmitting information obtained through the monitoring of the customer resource to the remote data center over the secure virtual connection.

The claimed distributed method for performing network monitoring that includes obtaining customer specific information from a remote data center over a first interface to an infrastructure management appliance, and establishing a secure virtual connection with the remote data center over a second interface to the infrastructure management appliance, is described throughout the instant application, for example, see page 6, line 25, to page 7, line 17, and Fig. 1, of the application. As shown

-13-

WEINGARTEN, SCHURCH,
GAGNER & LEBOVITZ LLP
TEL. (617) 542-2200
FAX. (617) 451-0313

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

in Fig. 1 of the application, an illustrative embodiment of the infrastructure management appliance 10 includes the first communication interface (not numbered) connected to a plurality of modems 18 associated with the remote data center 16, and the second communication interface (not numbered) connected to the customer network 12, which in turn is connectable to the public Internet 22. In the illustrated embodiment, the infrastructure management appliance 10 uses the secure virtual private network (VPN) 24 to communicate with the remote data center 16 through the Internet 22 over the second communication interface to the infrastructure management appliance 10 (see Fig. 1 of the application).

The Staveley reference discloses a data collection system 10 including a master machine 20 upon which a data collection program resides, and multiple target machines/devices 18. As shown in Fig. 1 of Staveley, the master machine 20 and the target devices 18 are connected together via a network connection 19 within a client site 12, and the master machine 20 is connected to a central site 14 via a communication connection such as the Internet 16. Significantly, the Staveley reference provides no teaching that the network connection 19 (the client network) is connectable to the public Internet 16. As indicated above,

-14-

WEINGARTEN, SCHURGEN,
GARDNER & LEBOVITZ LLP
TEL. (617) 643-2390
FAX. (617) 451-0333

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

amended claim 1 recites that the customer network is connectable to the public network (see also Fig. 1 of the application, which depicts the customer network 12 connected to the Internet 22). Because the customer network 12 is connectable to the Internet 22 within the claimed distributed network monitoring system, the local management station 14 connected to the customer network 12, the remote information center 32 connected to the Internet 22, and the remote data center 16 connected to the Internet 22, can each communicate with the infrastructure management appliance 10 over the second communication interface (not numbered) to the infrastructure management appliance 10 (see Fig. 1 of the application). In contrast, the target devices 18 connected to the network connection 19 and the devices 22 and 24 within the central site 14 connected to the Internet 16 communicate with the master machine 20 over separate communication interfaces (not numbered) to the master machine 20 (see Fig. 1 of Staveley).

Although the Examiner indicates on page 4 of the official action that Staveley discloses obtaining customer specific information over the first interface to the infrastructure management appliance (see column 9, lines 55-57; "client information is initially received over an HTTP interface"), and establishing the secure virtual connection with the remote data

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

center over the second interface to the infrastructure management appliance (see column 9, lines 55-57; "a secure connection is established over a secure interface (HTTPS/SSL)"), the Applicant respectfully points out that Staveley discloses the "HTTP interface" with reference to the data upload program of the client (see column 9, line 20, to column 10, line 11, of Staveley). As recited in amended claim 1, the infrastructure management appliance obtains customer specific information from the remote data center over the first interface to the infrastructure management appliance. In other words, the customer specific information is downloaded from the remote data center to the infrastructure management appliance over the first interface to the infrastructure management appliance. Because the "HTTP interface" is employed by Staveley in data upload operations, the "HTTP interface" of Staveley does not correspond to the first interface of amended claim 1, which can be employed by the claimed distributed network monitoring system in a data download operation. Like the "HTTP interface", Staveley also discloses the "secure HTTPS/SSL interface" with reference to the data upload program of the client (see column 9, line 20, to column 10, line 11, of Staveley). Both the "HTTP interface" and the "secure HTTPS/SSL interface" are therefore employed by Staveley in data

-16-

WEINGARTEN, SCHUBERT,
GARBERIN & LEBOVITZ LLP
TEL. (617) 542-2290
FAX. (617) 451-0311

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

upload operations over a connection to the Internet 16 (see also Fig. 1 of Staveley). In contrast, as recited in amended claim 1, the customer specific information is obtained from the remote data center over the first interface to the infrastructure management appliance, and the secure virtual connection is established with the remote data center over the second interface to the infrastructure management appliance.

Because the "HTTP interface" of the Staveley system is employed in data upload operations, and because the data upload operations performed by both the "HTTP interface" and the "secure HTTPS/SSL interface" of the Staveley system are performed over the connection to the public Internet 16 (see Fig. 1 of Staveley), the Applicant respectfully submits that the "HTTP interface" and the "secure HTTPS/SSL interface" disclosed in the Staveley reference do not correspond to the first and second interfaces to the infrastructure management appliance, respectively, as recited in amended claim 1. Accordingly, it is respectfully submitted that the Staveley reference does not teach or suggest all of the limitations of amended claim 1, and therefore the rejections of claim 1 and the claims dependent therefrom under 35 U.S.C. 102 should be withdrawn.

-17-

WEIDGARTEN, SCHURGEN,
GAYZEDIN & LESOVICI LLP
TEL. (617) 542-2290
FAX. (617) 451-0313

Application No. 10/010,915

Filed: December 7, 2001

TC Art Unit: 2144

Confirmation No.: 6110

In addition, for at least the reasons presented above with respect to amended claim 1, the Applicant further submits that the cited art of record including the Staveley reference does not teach or suggest all of the limitations of amended base claims 13 and 25, and therefore the rejections of claims 13 and 25 and the claims dependent therefrom under 35 U.S.C. 102 should be withdrawn.

Important advantages are obtained by providing a distributed system and method for performing network monitoring, in which customer specific information is obtained from the remote data center over a first interface to the infrastructure management appliance, and in which the establishing of the secure virtual connection with the remote data center is performed over the public network over a second interface to the infrastructure management appliance, as described and claimed in the instant application. For example, such customer specific information obtained from the remote data center over the first interface to the infrastructure management appliance can include parameters relevant to the establishment of the secure virtual connection subsequently established between the infrastructure management appliance and the remote data center over the second interface to the infrastructure management appliance (see page 7, lines 11-17,

-18-

WEDGECARTER, SCHORGIN,
GAGNEBIN & LEDOVICI LLP
TEL. (617) 942-2290
FAX. (617) 451-0323

Application No. 10/010,915
Filed: December 7, 2001
TC Art Unit: 2144
Confirmation No.: 6110

of the application). The Applicant respectfully submits that such an advantage is neither taught nor suggested in the Staveley reference.

The Examiner has rejected claims 2 and 14 under 35 U.S.C. 103(a) as being unpatentable over Staveley et al. in view of Liu (USP 6,079,020). The Applicant respectfully submits, however, that the Liu reference fails to cure the deficiencies of the Staveley reference, and therefore the Staveley and Liu references, whether taken alone or in combination, do not render dependent claims 2 and 14 obvious.

For example, like the Staveley reference, the Liu reference fails to disclose a distributed method for performing network monitoring that includes obtaining customer specific information from a remote data center over a first interface to an infrastructure management appliance, and, responsive to the customer specific information, establishing a secure virtual connection with the remote data center through a public network over a second interface to the infrastructure management appliance, as recited in amended claim 1.

The prior official action dated April 15, 2005 indicates that the Liu reference teaches obtaining customer information from a remote data center over a first interface, i.e., a VPN gateway, to

Application No. 10/010,915
Filed: December 7, 2001
TC Art Unit: 2144
Confirmation No.: 6110

an infrastructure management appliance, and establishing a secure virtual connection with the remote data center over a second interface, i.e., a public network interface via an Internet browser, to the infrastructure management appliance. The Applicant respectfully points out, however, that the Liu system merely employs the security features that exist in Internet browsers to provide security for communications between the VPN management station 160 and the VPN gateways 115, 125, 135, 145, 155 (see column 11, lines 38-45, and Fig. 1, of Liu). The Liu reference provides no hint that communications between the remote clients 140, 150 and the VPN management station 160 can be performed over first and second interfaces to the VPN management station 160 (see Fig. 1 of Liu).

Because the Liu reference fails to cure the deficiencies of the Staveley reference, the Staveley and Liu references, whether taken alone or in combination, do not render dependent claims 2 and 14 obvious. Accordingly, it is respectfully submitted that the rejections of claims 2 and 14 under 35 U.S.C. 103 should be withdrawn.

The Examiner has rejected claims 9 and 21 under 35 U.S.C. 103(a) as being unpatentable over Staveley et al. in view of Bhaskaran et al. (USP 6,601,084). The Applicant respectfully

Application No. 10/010,915
Filed: December 7, 2001
TC Art Unit: 2144
Confirmation No.: 6110

submits, however, that like the Liu reference, the Bhaskaran reference fails to cure the deficiencies of the Staveley reference, and therefore the Staveley and Bhaskaran references, whether taken alone or in combination, do not render dependent claims 9 and 21 obvious. Accordingly, it is respectfully submitted that the rejections of claims 9 and 21 under 35 U.S.C. 103 should be withdrawn.

In view of the foregoing, it is respectfully submitted that the present application is in a condition for allowance. Early and favorable action is respectfully requested.

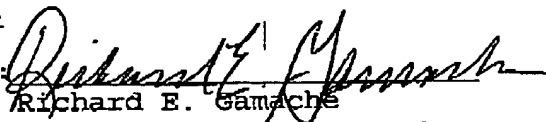
The Examiner is encouraged to telephone the undersigned Attorney to discuss any matter that would expedite allowance of

the present application.

Application No. 10/010,915
Filed: December 7, 2001
TC Art Unit: 2144
Confirmation No.: 6110

Respectfully submitted,

VIKRAM PILLAI

By: 
Richard E. Gama
Registration No. 39,196
Attorney for Applicant

WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
Ten Post Office Square
Boston, MA 02109
Telephone: (617) 542-2290
Telecopier: (617) 451-0313

REG/pjd
Enclosure

332227.1

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.